UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

106 S. ASH STREET, CARLSBAD, NM 88220 and

JUAN FLORES (YOB 1976)

Case No. 23-MR-619

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, attached hereto and incorporated herein by reference.

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 2422(b)	Coercion and enticement

The application is based on these facts:

See attached affidavit, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nancy Stemo, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephonically Sworn and Electronically Signed *(specify reliable electronic means)*.

Date: March 20, 2023

Judge's signature

City and state: Roswell, New Mexico

Barbara S. Evans, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: 106 S. ASH STREET, CARLSBAD, NM 88220, and JUAN FLORES (YOB 1976) MORE FULLY DESCRIBED IN ATTACHMENT A.	Case No. 23-MR-619

AFFIDAVIT

I, Nancy Stemo, having been duly sworn, does hereby depose and say:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2016. I am recognized as a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure ("FRCP") 41(a)(2)(C). I am currently assigned to the FBI's Child Exploitation and Human Trafficking Task Force where I investigate a myriad of federal violations including, violent crimes against children, human trafficking, child pornography, online enticement, and sexual exploitation of children. I have received on the job training from other experienced agents in the investigation of federal offenses, including the possession, distribution, and production of child pornography and enticement of a minor to engage in illegal sexual activity. My investigative training and experience includes, but is not limited to, conducting surveillance; interviewing subjects, victims, and witnesses; writing affidavits for search warrants and criminal complaints; collecting evidence; and learning legal matters, including the topics of fourth amendment searches. I have attended trainings specific to online child exploitation and human trafficking. I have previously participated in numerous child exploitation investigations and search warrants.

2. This affidavit is made in support of an application for a warrant to search under Federal Rule of Criminal Procedure 41 the premises located at 106 S. Ash Street, Carlsbad, New Mexico 88220, described further in Attachment A ("SUBJECT PREMISES"), for evidence, instrumentalities, and contraband described further in Attachment B, concerning coercion and enticement offenses, in violation of 18 U.S.C. § 2422(b).

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

RELEVANT STATUTES

4. Title 18 U.S.C. § 2422(b) provides in relevant part, "whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life." [1]

[1] It is also a violation of this statute to attempt to induce a minor through an intermediary who appears to the defendant to exercise some degree of control over that minor, such as a parent or a babysitter. *United States v. Murrell*, 368 F.3d 1283 (11th Cir. 2004). [M]any …circuits that have held that a defendant violates § 2422(b) by communicating only with an adult intermediary if the defendant's communications with that intermediary are intended to persuade, induce, entice, or coerce the minor child's assent to engage in prohibited sexual activity. *United States v. Roman*, 795 F.3d 511, 516 (6th Cir. 2015)k; *United States v. Hite*, 769 F.3d 1154, 1160 (D.C.Cir.2014); *United States v. Berk*, 652 F.3d 132, 140 (1st Cir.2011); *United States v. Douglas*, 626 F.3d 161, 164 (2d Cir.2010) (*per curiam*); *United States v. Nestor*, 574 F.3d 159, 161–62 (3d Cir. 2009); *United States v. Caudill*, 709 F.3d 444, 446–47 (5th Cir.), cert. denied,, 133 S.Ct. 2871, (2013); *United*

5. New Mexico State Code Section 30-9-11 makes it a State of New Mexico crime for any person to unlawfully and intentionally cause a person under thirteen years of age to engage in sexual intercourse, cunnilingus, fellatio, or anal intercourse or causes the penetration, to any extent and with any object, of the genital or anal openings of another, whether or not there is any emission.

6. New Mexico State Code Section 30-9-13 makes it a State of New Mexico crime for any person to unlawfully and intentionally touch or apply force to the intimate parts of a minor, under the age of thirteen, or unlawfully and intentionally cause a minor, under the age of thirteen, to touch one's intimate parts. "Intimate parts" means the primary genital area, groin, buttocks, anus or breast and includes touching of the intimate parts of the minor over the minor's clothing.

DEFINITIONS

7. The following terms are relevant to this affidavit in support of this application for a search warrant:

a. *Child Pornography*: The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in

---

States v. McMillan, 744 F.3d 1033, 1036 (7th Cir.), cert. denied, 135 S.Ct. 292; *United States v. Spurlock*, 495 F.3d 1011, 1013–14 (8th Cir.2007); *United States v. Lanzon*, 639 F.3d 1293, 1298–99 (11th Cir.2011).

sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 and 2256(2), (8).

b. *Computer*: The term "computer" refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, mobile phones, and devices. *See* 18 U.S.C. § 1030(e)(1).

c. *Electronic mail ("e-mail" or "email")*: "E-mail" refers to a method of exchanging digital messages from an author to one or more recipients. Users may attach digital media to their e-mails. Modern e-mail operates across the Internet or other computer networks. E-mail systems are based on a store-and-forward model. E-mail servers accept, forward, deliver and store messages. E-mail accounts may be accessed by computers, to include smartphones and tablets.

d. *Internet*: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

e. *Internet Protocol ("IP") Address*: An "IP address" is a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that

Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

f. *Internet Service Providers ("ISPs")*: "ISPs" are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. *Minor*: The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

h. *Sexually Explicit Conduct*: The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

i. *Smartphone*: A "smartphone" is a type of mobile or cellular telephone, and functions as multi-purpose mobile-computing devices. Smartphones can function as traditional telephones with the additional ability to store contact

information, send and receive voice, text, and media messages, store information and media, access the Internet, and perform many of the same functions as a traditional computer. A smartphone user may perform these various functions through software applications ("apps") which may store evidence of such use on the device.

j. "*Records*," "*documents*," *and* "*materials*": These terms include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

DETAILS OF THE INVESTIGATION

8. On November, 8, 2022, a Task Force Officer ("TFO") was working as an Online Covert Employee ("OCE") with the Metropolitan Police Department, Washington, D.C. and Washington Field Office ("WFO") Child Exploitation and Human Trafficking Task Force. As an OCE, the TFO entered a foreign fetish website, hereinafter "Website 1." The OCE is aware that website is used to meet, discuss, and trade images, links, and videos containing child pornography. The OCE has been a member of the website for over a year. A Website 1 user, "Reahoe," initiated a private chat with the OCE within Website 1. As will be explained in further detail below, "Reahoe" was subsequently identified as Joseph Crutcher, who admitted to portraying his wife, Rachel Crutcher, on the website.[2]

9. Affiant learned that Joseph and the OCE exchanged numerous messages on Website 1 discussing the sexual exploitation of children. Joseph claimed to be a "taboo mommy," and advised he had access to a nine-year-old child whom he "shared and love[d]

[2]Joseph Crutcher will be referred to as Joseph and his wife, Rachel Crutcher, will be referred to as Rachel to avoid confusion since they share a last name.

to lick cum off her mound." Joseph sent various images of a female minor, (hereinafter Jane Doe 1) to the OCE. Joseph sent an image to the OCE in which Jane Doe 1's shorts were pulled down and her bare vagina was visible. The child's hand was down her pants, and her fingers were near or on her vagina. The child is pre-pubescent. Your affiant has personally reviewed the image and believes it is lascivious display of a minor's genitals, constituting child pornography.

10. On November 9, 2022, an administrative subpoena was served on Website 1 for subscriber information for "Reahoe." On the same date, Website 1 responded and provided the email, crutcherjoe3@gmail.com, a self-provided date of birth of April 17, 1985, and IP logs spanning the length of the account. The IP logs were reviewed and there was a combination of T-Mobile wireless and Windstream Communications IP addresses. An exigent request for records was submitted to Windstream Communications for IP address 67.141.33.221. On November 10, 2022, Windstream Communications responded and provided the service address as a specific address in Carlsbad, New Mexico, and the subscriber as Rachel Crutcher.

11. The FBI conducted queries of available commercial, law enforcement sensitive, and open-source databases with the information obtained from Website 1, namely the email crutcherjoe3@gmail.com and DOB 4/17/85 and identified Rachel and Joseph as possible subjects. A review of Rachel's Facebook profile showed a picture of Jane Doe 1 with Rachel and Joseph.

12. On November 9, 2022, the FBI obtained and executed a search warrant on Rachel and Joseph's residence, in Carlsbad, New Mexico. The search warrant authorized

law enforcement to search electronics capable of connecting to the internet. Jane Doe 1, Jane Doe 2, and another minor child were present at the residence.

13. After being advised of his *Miranda* rights and waiving his rights, Joseph stated he took the pictures of Jane Doe 1 sent to the OCE and had sent the photos to other unknown individuals via Website 1, Wickr, and Kik. Through training and experience, I am aware Wickr and Kik are messaging platforms that are accessible via an Internet-based application. Wickr is an encrypted service. Both applications have been associated with the possession and distribution of child pornography material. Joseph stated he portrayed himself online as his wife, Rachel. Joseph claimed he only took photographs of Jane Doe 1 because that was the only way he could ejaculate. Joseph stated he, Rachel, and his children traveled to a nude hot spring in New Mexico and some of the photos were taken there. Joseph denied sexually abusing Jane Doe 1 or other minors. On that date, Rachel was interviewed but denied awareness or involvement in any sexual abuse of Jane Doe 1, Jane Doe 2, or other minors.

14. On November 10, 2022, a child forensic interviewer interviewed Jane Doe 1 and Jane Doe 2. Jane Doe 1 reported being nine years old and stated Joseph and Rachel sexually abused her by sticking their fingers into Jane Doe 1's vagina, receiving oral sex from Joseph, and Joseph taking photos of her while she was naked. Jane Doe 1 disclosed Joseph would text his friends on an app and ask them to join him. A few months ago, in approximately September 2022, Jane Doe 1 said she was taken to a park by Joseph, and they met with a man she referred to as "Juan." The law enforcement officer who observed the forensic interview recognized the park Jane Doe 1 described as Carlsbad Municipal Beach in Carlsbad, New Mexico. Jane Doe 1 recalled Joseph and Rachel had sex with Juan

and on one occasion, Juan asked Jane Doe 1 to touch his penis, but she refused. Jane Doe 1 said she had not seen Juan in several months as Joseph and Rachel had moved on to other men. Jane Doe 1 also made other disclosures regarding sexual abuse by other individuals that have been corroborated by law enforcement.

15. Jane Doe 2 is five years old and did not make any disclosures regarding sexual abuse.

16. On November 10, 2022, forensic examinations of Joseph and Rachel's Samsung Galaxy A12 cell phones were initiated. During a preliminary review of the devices, several images of Joseph and Rachel with Jane Doe 1 and Jane Doe 2, were observed in which everyone was nude. The images included photos sent to the OCE of Jane Doe 1 on Website 1. Additional nude images of Jane Doe 1 and Jane Doe 2 were also located. I am aware the Galaxy cell phones were manufactured in Vietnam.

17. On November 10, 2022, Rachel was re-interviewed. After being advised of her *Miranda* rights and waiving those rights, Rachel admitted she and Joseph sexually abused Jane Doe 1, Jane Doe 2, and another minor victim who the two had access to since birth. Rachel stated the abuse was consistent and constant. Rachel advised she was threatened and abused by Joseph if she did not do what she was told and was forced to lick Jane Doe 1's and Jane Doe 2's vaginal areas. Rachel admitted to penetrating Jane Doe 1's vagina with her fingers within the last couple months. Rachel has participated in sexual acts with Jane Doe 1 on at least a dozen occasions and with Jane Doe 2 on at least one occasion. Rachel stated she was forced to take photos with Joseph, Jane Doe 1, and Jane Doe 2 while engaged in sexual acts.

18. Additionally, Rachel reported Joseph found a man online known as "Juan." She did not believe Juan touched Jane Doe 1 or Jane Doe 2, who were both present during sexual interactions with Juan. Rachel said that during one of the interactions with Juan, Joseph performed oral sex on Jane Doe 1.

19. On November 10, 2022, Joseph was re-interviewed. After being advised of his *Miranda* rights and waiving those rights, Joseph was advised that Jane Doe 1 and Jane Doe 2 had been interviewed along with Rachel. Joseph admitted to sexually abusing Jane Doe 1 and Jane Doe 2 with Rachel. Joseph stated he forced Rachel to do things she did not want to do but denied physically abusing her and instead would threaten to leave her if she did not do what he asked of her. Joseph admitted to using various Internet based applications and websites to interact with people, including Fetlife, Kik, Wickr, Telegram, and XHamster. Joseph admitted he had sent several nude photographs of Jane Doe 1 and Jane Doe 2 to unknown individuals on these platforms. Joseph said he generally pretended to be Rachel on these platforms. Joseph indicated there was another occasion in which he discussed sexual matters with an individual he met online via Website 1 that turned out to be his former boss. Joseph knew him only as "Juan," and both had previously worked at Walmart. Joseph met with Juan on three occasions. Joseph said the first time they met, Rachel and Juan played Pokémon together. He said the second time they met, Rachel masturbated Juan while Jane Doe 1 and Jane Doe 2 were present. Joseph said the third time they met, Joseph performed oral sex on Jane Doe 1, but specifics on the third occasion were unclear.

20. Law enforcement obtained a search warrant for the Website 1 account, "Reahoe," which was being utilized by Joseph. The communications on that account were

reviewed for evidence of child sexual exploitation. Joseph was in communication with dozens of individuals and discussed sexual exploitation of children with approximately two dozen individuals, one such individual utilized the username, "fluffydragon28."

21. On December 16, 2022, an administrative subpoena was served on Website 1. Website 1 provided the following information for Fluffydragon28:

Email: jflores.morco@gmail.com

DOB: **/**/1976

Phone Number: 575-973-****

22. A check of a law enforcement database showed the likely subscriber of the phone number, 575-973-****, was JUAN ANTONIO FLORES, YOB: 1976, with associated email jflores.morco@gmail.com.

23. On December 23, 2022, an administrative subpoena was served on Google for the email, jflores.morco@gmail.com. Google provided the following information:

Billing Name: Juan Flores

Phone number: 575-973-****

Billing Address for Paypal Account: 106 S. Ash, Carlsbad, NM 88220

24. An open-source query of jflores.morco@gmail.com was conducted and a photo of a male was associated with the account was located. A query of the New Mexico Motor Vehicle Division's ("NM MVD") records for Juan FLORES with a DOB 8/28/1976 was conducted and a photo of FLORES was obtained. The male in the photo of jflores.morco@gmail.com and the photo provided by the NM MVD were of the same male.

25. On December 20, 2022, an administrative subpoena was served on Verizon Wireless and the FBI was informed the service provider was TracFone. No subscriber information was available for 575-973-****.

26. An employment check on FLORES showed he was formerly employed at Walmart from 2017 to 2019. In August 2019, FLORES submitted a New Mexico Department of Workforce Solutions unemployment application and listed the SUBJECT PREMISES as his address, the phone number 575-973-****, and email jflores.morco@gmail.com. FLORES is currently employed at a Lowes Home Improvement and has been since 2019.

27. FLORES listed the SUBJECT PREMISES as his residence on his New Mexico driver's license. An open-source query, and a law enforcement database query, of FLORES' name and Carlsbad, NM showed 106 S. Ash Street, Carlsbad, NM was his residence. On November 15, 2022, deputies from the Eddy County Sheriff's Office conducted surveillance at the SUBJECT PREMISES in an attempt to identify FLORES. A Pontiac Vibe, license plate AGTP26, registered to Juan Antonio FLORES, DOB 8/28/76, was parked at the residence. The vehicle was registered to the SUBJECT PREMISES.

28. The FBI obtained a New Mexico driver's license photo of FLORES and compared it to photos of Fluffydragon28's pictures on Website 1. The FBI also served Website 1 with a search warrant for Fluffydragon28's Website 1 account. Several photos of the user were provided in the search warrant return. I believe the photos posted on the Fluffydragon28 are of FLORES, and FLORES is the user of Fluffydragon28.

4. Joseph[3] and FLORES began communicating on Website 1 on or about September 7, 2022. On September 10, 2022, FLORES asked what the youngest Joseph had ever played with was. Joseph expressed hesitancy and instead asked FLORES several questions, including what his youngest was. They briefly discussed other sexual activity and FLORES again asked, "so how young was it" and Joseph replied "5." FLORES wrote, "what all did you do," "you not a bad person," and Joseph said he "licked her." FLORES continued to ask about the encounter, including who the child was, whether the abuse was ongoing, and how old she was currently. Joseph indicated being nervous talking about it, and FLORES wrote, "everything stays between us," "tell me more. It's a turn on for me," and "she the only one you've done that with?"

29. The two continued to discuss sexual activities and planning an in-person meeting. After discussing meeting in person, the following conversation ensued:

FLORES: How often do others play with her? How often does she ask for it?[4]

Joseph: We will see how it all goes when we meet. Not as much as we all would like

FLORES: Does she walk around naked. Does she watch you sucking and fucking guys?

Joseph: At home yes she likes being naked. Yes she has a lot.

FLORES: Does she get real close

Joseph: Sometimes yes

FLORES: Nice. Where do they cum on her? Where do you like cum on you

[3] Based on the context of most of the messages sent by Fluffydragon28, the user mistakenly believed he was communicating with Rachel. Except for a few instances, Joseph allowed Fluffydragon28 to believe Rachel was the user of the account and rarely informed Fluffydragon28 he was responding to the messages.

[4] I believe based on the conversation that "her" refers to Jane Doe 1. Often throughout their conversations, FLORES and Joseph refer to "she" or "her" when discussing Jane Doe 1.

Joseph: Cum on or in for me her pussy cum on mound or I hold it open to cum in

FLORES: Wow that's hot

Joseph: It is very hot

FLORES: Need to shower and stroke my hard cock now

Joseph: Mmmmm hard from what ? I'm dripping wet

FLORES: You and what you do with her

Joseph: That's hot

FLORES: Just thinking of her naked walking around

Joseph: She does it all the time

FLORES: Her sitting on my lap with my cock pressed against her ass

Joseph: Mmmmmm sexy. Want her in a dress no panties

FLORES: Rubbing her little nipples. When we meet?

Joseph: yesss

FLORES: Sure. Will i be able to touch her when we meet or just look at her?

Joseph: It will be up to her.

FLORES: Of course. What does she do when she wants to be touched?

…

Joseph: She will let you know know

30. On September 10, 2022, FLORES wrote, "the only thing close that ive done close to that is just seen naked photos and videos of less than 18 and women with animals." The two continued discussing an in-person meeting, and the following conversation ensued:

FLORES: What all are you looking from me?

Joseph: I like watching men make love and.fuck

FLORES: Don't know if I will do anything with your hubby

Joseph: That's ok

FLORES: Are you hoping she wants me to touch her? Do some of the guys fuck you too after hubby?

Joseph: Yes I have shared dick with him before maybe.just a little hoping she wants you to touch her[5]

31. On September 11, 2022, the following conversation ensured between Joseph and FLORES:

FLORES: Horny thinking of you and her wearing dresses and no panties

Joseph: Tonight you can see it. And maybe feel it.

FLORES: Only if you say i can to you and she tells me i can to her

Joseph: So around 7:30 tonight

FLORES: Lower tansil?

…

Joseph: Yes lower tansil

…

FLORES: At the little playground?

Joseph: Yea at veterans park

FLORES: Im excited and nervous

Joseph: Same here

FLORES: Sit at the bench area next to playground?

[5] Based on the context of the conversation, I believe user FLORES continued to believe he was communicating with Rachel and the reference to "her," was to Jane Doe 1, and "hubby," was Joseph.

32. On September 12, 2022, the following conversation ensued between Joseph and FLORES:

FLORES: Would have licked her fingers after she was playing with her pussy instead of wiping it on your forehead

Joseph: So did you have fun

FLORES: Yes i did. Would tues or wed work for you? Will it be just you coming over to hotel? Or hubby and or daughter too?

Joseph: Probably hubby not sure about her but most likely. Wednesday is good.

FLORES: Kept seeing your tits while sleeping last night and feeling tour wet pussy. Plus the images of her showing her ass on the swing and her rubbing her pussy and smearing it on your forehead. Was hoping she would have sat on the table in front of me showing her pussy waiting for me to look, touch, and or taste her. I dont mind sitting out there and visiting again. Or somewhere else that has a playground or something. Dont mind just talking and fingering you out in public lol

Joseph: We.can do that too. I enjoyed myself last night. And she.is just a little shy maybe she'll open up next visit

FLORES: What all do you want Wednesday? Im glad you enjoyed last night. I really wasnt expecting her to do everything that she did. That was a big suprise. Can i kiss you? Does she like kissing? What all did you and brother do when you were that age? Besides brother and daughter any other family play with you?

Joseph: This is joe she is at.work. I'm cool with you doing what ever to both

33. On September 13, 2022, the following conversation ensued between Joseph and FLORES:

FLORES: Fuck more nasty dreams of the two of you

Joseph: That's hot

FLORES: You and [Jane Doe 1] are going to make me crazy lol

Joseph: That's sooo sexy

FLORES: Yea. Eating her pussy while you're sucking my dick.

34. On September 14, 2022, and into September 15, 2022, the following conversation ensued between Joseph and Flores:

FLORES: Fuck those nasty dreams. Want to lick that pussy and lick and suck on those titties

Joseph: Mmmmmm what kind of dream

FLORES: Licking [Jane Doe 1] pussy then yours while she is laying on top of you. Other was you and her sucking my dick together. You showing her how it's suppose to be done. Then one night you invited me to come watch other guys play with her as you hubby and i watched then took care of her after they left

Joseph: That one is very hot

FLORES: Like I've had thoughts before about girls [Jane Doe 1's] age but nothing like I've been thinking of since we started talking. Just want to taste her and taste you to compare over and over and over again. Being able to touch her and feel my cock against her pussy and ass. To feel her nipples against my lips and tongue. The thought of having pictures of her to jackoff to everyday when she pops in my head. To look at her and you as i stroke my dick anytime I want

Joseph: Really really like how perverted you are

FLORES: You brought it out of me. Your experiences and then seeing [Jane Doe 1] fuck it just has me going.

Joseph: Kinda looking forward to licking your.cum off her

FLORES: Just kinda

Joseph: Ok kinda alot

FLORES: Mmmmm that's better. Want to taste her pussy juices and lick her clit and lick and suck her nipples. Feel her sitting on my cock while i touch her.. after daddy fucks her I would like to feel her pussy wrapped around my cock

Joseph: Tell me what dark sexual things do you want.to do with my family. That's hot.

FLORES: Since [Jane Doe 1] is the only horny nudiest walking around. Want to have a foursome where we are all licking and sucking on her. Dad and i are filling her holes at the same time. You cleaning our dicks off eat time we take it out of her pussy. [Jane Doe 1] eating your pussy while you are sucking me or hubby and the other is fucking [Jane Doe 1]. Ive done it before but need to be in right mind set but

would bend daddy over and fuck his ass as a thank you for giving me honor of play with [Jane Doe 1] and you. Fist your pussy to make you squirt all over the place. Me and hubby filling your holes and [Jane Doe 1] cleaning our dicks after they have been in your pussy .... then one day be allowed to take [Jane Doe 1] with me wherever for a few hours or so to play with her alone then bring her back with cum in her holes for you and hubby to lick and suck out of her... Allowing me to take pictures or you sending me pictures of you and [Jane Doe 1] naked together. Show me every hole. Showing me everything that I can have when we are able to meet. To have so i can stroke and think of both of you. This old man stoking hard cock to those younger than i

Joseph: Mmmmm hot you going share her and bring home multiple creampies

FLORES: If it is allowed by you and hubby yes

Joseph: Mmmmmm sexy

FLORES: Everything i do will always be by your rules

…

FLORES: Will she be around every time I get to see you

Joseph: That's up to you and her

FLORES: And after daddy gets her i can't wait to be able to put my dick inside both of you

Joseph: It's going.to be.fun

FLORES: Would love her there each time if she wants

Joseph: We will see

35. On September 18, 2022, and into September 19, 2022, the following conversation ensued between Joseph and FLORES:

FLORES: We are at lower t chatting like last time but [Jane Doe 1] decides to sit on the table with her back to me so i can reach under her leg to rub on her pussy. Her pussy is staight in your face. I brought a little vibrator just in case. I reach into my pocket to get it out. Turn it on and place on her smooth beautiful pussy. Little by little i get it right on her little clit. While holding the vibrator steady with one hand the other is wrapped around her body to keep.her still and comfortable. You can till she is about to cum from the vibrations. You keep looking at the wetness that i am causing that you decide to look closer. As you move in closer she begins

to cum not only does she cum hard but she starts to squirt all over your face. Pull you closer soni can lick that off your face. Then i turn her around soni can clean up the big fucking mess i made on her.

Joseph: That's hot. Sorry been in the mountains.

FLORES: It's all good. I understand. Next time we meet at lower t i want to sit next to you so i can at least finger fuck that wet pussy of yours. Finger fuck you till you are squirting all over the bench and ground.

36. On September 20, 2022, the following conversation ensued between Joseph and FLORES:

FLORES: You riding my cock as [Jane Doe 1] sits on my face. Licking her little pussy and sucking on her clit. Then you sitting on my face so i can eat that hairy pussy while she strokes my hard cock.

Joseph: Want to meet Friday evening lower t

FLORES: Sure thing. Same time? You been able to find more sex partners in town?

Joseph: Yea around 7:00 7:30. No not yet. Not anyone to play with no

FLORES: That sucks. I want your body. [Jane Doe 1] is a bonus. A special bonus.

Joseph: Yesssss she is.

37. On September 23, 2022, the following conversation ensued between Joseph and FLORES:

Joseph: Still on for tonight?

FLORES: You wearing a dress again?

Joseph: Probably

FLORES: I hope you do so i can finger fuck you

Joseph: I'm sure the 3 of us girls will be in dresses[6]

FLORES: Does the other play too?

[6] I believe the third person Joseph is referring to is five-year-old Jane Doe 2.

Joseph: Only when she wants it

FLORES: Nice...i thought it was only [Jane Doe 1]. Even more naughty thoughts to think about

Joseph: Yea what's that

FLORES: Licking all three pussies. Feeling my cock along those pussies. Three asses to be sitting on my cock. Sucking and licking three sets of titties.

38. On September 24, 2022, and into September 25, 2022, the following conversation ensued between Joseph and FLORES:

FLORES: I did enjoy stroking my cock while [Jane Doe 1] was watching. It's okay that she didn't want me touching or licking her. More we get to see each other the more she will get comfortable with me. I'll get more comfortable too so my cock will be full hard for you. It's all new to me and it's a taboo that I've pretty much have wanted to do. I enjoy touching you and fingering you.

Joseph: I really enjoyed myself tonight

FLORES: Thank you for another great evening. Dont feel bad that you were hurting and not in the naughty mood. It's all good. The naughtiness is a bonus. It was nice see3her little pussy while you were tickling her. I really do enjoy hanging out with you guys. Last time you said the girls like me. What did they say that let you know that they do?

39. On September 29, 2022, FLORES sent Joseph a message that said, "Lick your pussy and [Jane Doe 1's] pussy tasting that mother daughter sweetness."

40. On October 11, 2022, FLORES asked how they were and specifically mentioned Jane Doe 1 and Jane Doe 2 by name. On October 15, 2022, FLORES wrote, "need my mouth on those nipples and on [Jane Doe 1's]." On October 26, 2022, FLORES indicated he wanted to hang out with them again. The last message received from FLORES was on November 10, 2022, and FLORES inquired about Joe and the girls.

41. A Samsung cell phone attributed to Rachel was seized during the federal search warrant that was executed at the Crutcher's residence. A review of that device's

contents showed FLORES' phone number, 575-973-****, was saved in Rachel's contacts as "Juan Fb." There were text messages between Rachel and FLORES that began on September 12, 2022, and ended on September 25, 2022. On September 12, 2022, FLORES wrote, "very nice wet pussy." On September 14, 2022, FLORES wrote, "No go tonight. Might be able to meet you later if you go Pokémon hunting." On September 25, 2022, FLORES inquired if they were still on for the night and Rachel indicated they were.

42. A query for FLORES' history with the New Mexico Child Youth and Families Division ("CYFD") yielded a 2011 unsubstantiated report alleging sexual molestation of a female relative. At the time of the report, the child was eight years old.

43. On March 13, 2023, FBI re-queried FLORES' driver's license and vehicle registration through NM MVD. Both continued to show his address as 106 S. Ash St., Carlsbad, New Mexico, 88220. On March 16, Carlsbad Police Department drove by 106 S. Ash St., Carlsbad, New Mexico, 88220, and noticed the home appeared to look the same, although no vehicles were parked outside. On March 20, 2023, FBI re-ran FLORES through numerous databases, including open-source databases and a law enforcement database. All databases continued to show his address as 106 S. Ash St., Carlsbad, New Mexico, 88220. On March 20, 2023, Carlsbad Police Department again drove by the residence, which appeared the same, but again no vehicle was outside.

44. It is unknown if anyone other than FLORES resides at the SUBJECT PREMISES. However, this warrant only seeks authorization to seize and search items believed to belong to FLORES or to which FLORES had access.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

45. I have both training and experience in the investigation of computer-related crimes. Based on my training and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs and/or videos.

c. A device known as a "modem" allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media

of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which plug into a port on the computer – can store thousands of images and/or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Individuals can easily store, carry or conceal media storage devices on their persons. Individuals also often carry smartphones and/or mobile phones on their persons.[7]

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user's computer, smartphone or external media in most cases.

[7] *See United States v. Carpenter,* 138 S. Ct. 2206, 2218 (2018) (noting that individuals "compulsively carry cell phones with them all the time."); *see also Riley v. California,* 134 S. Ct. 2473, 2490 (2014) (referencing a poll finding that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time…").

46. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

47. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, this warrant would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

48. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe the records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge and training, I know that forensic examiners can recover computer files or remnants of such files months or even years after they have been downloaded onto a storage medium, deleted, or viewed

via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how an individual has used a computer, what the person used it for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that an individual viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

49. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which the computer created them, although it is possible for a user to later falsify this information.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude

the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when someone accessed or used the computer or storage media. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files,

along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records sought, a review team cannot always readily review computer evidence or data in order to pass it along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a person used a computer, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because someone used it as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training, I believe that a computer used to commit a crime of this type may contain evidence of how FLORES used the computer; sent or received data; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

50. Based upon my training and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by

corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures, which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted. Further, the examination may employ techniques that would damage or destroy the device, but result in a forensically sound copy of data stored on the device;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

51. Additionally, based upon my training and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual

to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password). Wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

52. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

53. Because several people may share the SUBJECT PREMISES, it is possible that the SUBJECT PREMISES, will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. This warrant does not seek authorization to seize or search anything unless it is believed it belongs to FLORES or to which FLORES had access.

BIOMETRIC ACCESS TO DEVICES

54. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

a. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

b. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the

front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

c. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not

known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Therefore, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request permission to: (1) press or swipe the fingers (including thumbs) of FLORES to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the face of FLORES and activate the facial recognition

feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of FLORES and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that FLORES state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to ask FLORES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

INTERSTATE NEXUS

55. I believe that the element of "any facility or means of interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. § 2422(b), for the limited purpose of securing a search warrant.

56. Website 1 is a website that utilizes the Internet, and thus is a facility or means of interstate or foreign commerce.

57. Additionally, TracFone Wireless is a subsidiary of Verizon Wireless. Verizon Wireless is a nationwide cellular network. In order to send or receive text messages, a device utilizing TracFone Wireless is required to connect to the nationwide cellular network or the internet, both of which are a facility of means of interstate or foreign commerce.

CONCLUSION

58. Based on the information set forth above, there is probable cause to believe that items more fully described in Attachment B and consisting of evidence, contraband,

instrumentalities and/or fruits of violations of 18 U.S.C. § 2422(b), will be found at the location more fully described in Attachment A. Further, based upon the foregoing paragraphs, judicial authority is specifically requested to complete the search/examination of the seized items at an appropriate law enforcement facility.

59. Assistant United States Attorney Matilda McCarthy Villalobos has reviewed and approved this application.

60. I swear that this information is true and correct to the best of my knowledge.

SPECIAL AGENT NANCY STEMO
FBI

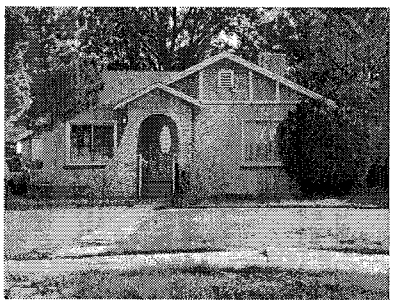
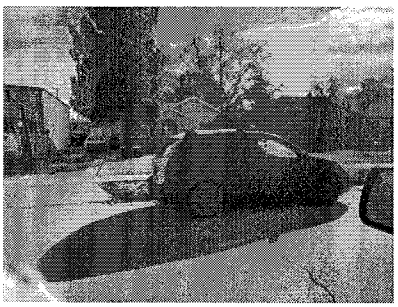
Electronically Subscribed and Telephonically SWORN to before me this 20th day of March, 2023.

The Honorable Barbara Smith Evans
United States Magistrate Judge

ATTACHMENT A

The property to be searched is described as follows:

1. The entire property located at 106 S. Ash Street, Carlsbad, New Mexico, 88220, including the residential building(s), any outbuildings, any appurtenances, and the surrounding curtilage ("SUBJECT PREMISES") in which FLORES lives or has access to. The SUBJECT PREMISES appears to be a single-family residence that is tan in color and has a white front door. There is also a detached garage that may have been converted, either partially or fully, into a residence, although it is unclear if anyone resides in the possibly converted garage as the building sits behind the primary residence and the interior cannot be seen from the street. There are no posted numbers on the residence or curb. None of the buildings are clearly labeled indicating they are separate residences or separately inhabited (i.e., none of the buildings are labeled with "A" and "B," as would be expected if the building were inhabited by different individuals).

2. The person of Juan FLORES (DOB 8/28/1976) provided that this person is located at the subject premises and/or within the District of New Mexico at the time of the search.

3. During the execution of the search of the premises described in Attachment A, law enforcement personnel are also specifically authorized to compel FLORES to provide biometric features, including pressing fingers (including thumbs) against and/or putting a device in front of a face, or any other security feature requiring biometric recognition, of:

    a. any of the devices found at the premises, and
    b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

    for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the premises to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device.

This warrant does not authorize law enforcement personnel to require that FLORES state or otherwise provide the password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

ATTACHMENT B

All records relating to violations of 18 U.S.C. § 2422(b) relating to the enticement of a minor by Juan FLORES, which constitute evidence of the commission of the criminal offense, contraband, the fruits of the crime, or property designed or intended to use or which is or has been used as the means of committing a criminal offense, including:

1. Computers or storage media used as a means to commit the violations described above.

2. All visual depictions (including images, videos, negatives, still photos, video tapes, artists drawings, slides, and any type of computer formatted file) which depict a minor engaged in sexual conduct, or the lewd exhibition of genitalia, or posed or candid in a sexual manner, including clothed or partially clothed.

3. All non-sexual photographs of minors who may be the subject of the visual depictions described in paragraph 1 of this attachment, or the victim of other child exploitation offenses or attempted offenses as described above, and any information, including names, addresses, nicknames, schools, or after-school groups, that may lead to the age or identity of any minor depicted in any visual media seized.

4. Any correspondence with minor children, including correspondence that may be used to identify the child, or demonstrate an effort to groom, meet, or sexually exploit the child.

5. Any correspondence with others related to efforts to groom, meet, or sexually exploit children.

6. Any correspondence with others related to any sexual interest in children.

7. All copies and originals of envelopes, letters, diaries, ledgers, journals, chats and other correspondence pertaining to the possession, receipt, distribution, production, and/or reproduction of visual depictions of a person under the age of 18 years engaging in or simulating sexual conduct, or pertaining to other sexual crimes against children.

8. All materials or items which may be sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such materials includes written materials dealing with child development, sex education, child

pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, journals and fantasy writings.

9. All documentation, (whether on paper or stored magnetic, digital, or optical media) describing discussions by any individual or entity concerning: the identity of persons that are sexually attracted to children, members of child sex advocacy groups, child victims and other persons involved in the sexual exploitation of children.

10. All documentation and records, showing discussions by any individual or entity concerning: the selling, licensing, manufacturing, marketing, transferring, providing, furnishing, sampling, or examining of documents, records, images, magnetic media or other items incorporating, or purportedly compatible with the producing, sending, receiving, possessing and viewing of child pornographic materials.

11. All records showing the acquisition and/or sale of computer hardware, computer software, or computer documentation that explains or illustrates how to configure or use computer hardware, and communication programs.

12. All documentation related to computer passwords, encryption keys, and other access devices.

13. All computer hardware equipment, connector cables, and corresponding logs (including: central processing units, monitors, modems, routers, keyboards, printers, computer scanner equipment and or video transfer equipment).

14. All storage devices (including: external and internal hard drives, cell phones, "smart" phones, and PDA's capable of sending and receiving images and/or text messages, thumb drives, cartridge tapes, magnetic tapes, optical and digital storage devices, digital cameras, CD's, DVD's, memory cards, Micro SD Cards, iPods, X-Box, PSP players, video game consoles, floppy disks or other media capable of storing data).

15. All computer software stored on hard disks, digital, optical, and magnetic media devices, and floppy disks containing computer programs, including software data files, electronic mail files, instant message files, software programs and files to receive and or transmit photographs, and operating logs and instruction manuals relating to the operation of the computer hardware and software to be searched.

16. All computer related manuals, textbooks, computer print outs, and other documents used to access computers and record information taken from computers.

17. All documents, web history, and communications demonstrating any communication or correspondence with any person or groups of persons supplying,

distributing, or trading in child sexual abuse materials, or discussing a sexual interest in minors, including communications with individuals purporting to be under the age of 18.

18. Bookmarks, internet history, temporary internet files, .lnk files, cache files, and other items showing how the computer was accessed, who accessed the computer, and/or how the computer was utilized;

19. All accounts or records evidencing manufacturing, production, distribution, receiving, possessing, or sales of printed and photographic materials, negatives, film slides, digital images, motion pictures, video tapes and documents relating to sexual conduct of persons under the age of 18.

20. Articles of personal property tending to establish the identity of person or persons having the dominion and control over the computer equipment, cellular telephone, or digital media.

21. All safes or lock boxes, where diaries, notes, journals, pictures or other evidence of crimes against children may be stored for safekeeping against seizure.

22. All evidence related to all off-site storage units, other residences, safety deposit boxes, etc. where diaries, notes, journals, pictures or other evidence of crimes against children may be stored for safekeeping against seizure.

23. All cellular telephone records to establish ownership of the device or the residence.

24. All contracts, agreement records and accounts with Internet providers, computer bulletin boards, or other computer online service provider.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI shall deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.